PAYMENTS INDUSTRY INTELLIGENCE
Payments
CARDS & MOBILE

PAYMENTS CARDS AND MOBILE RESEARCH

PSD2 and Europe's Open Banking Mandate – Challenges for Banks and FinTechs

NCR

PSD2 and Europe's Open Banking Mandate – Challenges for Banks and FinTechs

Contents

Principal Author
Horst Foerster horst@paymentscm.com

Contributing Writers
Alex Rolfe alex@paymentscm.com
Andy Brown andy.brown@ncr.com

PSD2 and Europe's Open Banking Mandate – Challenges for Banks and FinTechs

1.1 EXECUTIVE SUMMARY

The adoption of the revised Payment Services Directive (PSD2) is formalising the relationship between Banks and FinTechs by establishing Open Banking, providing open access to customer account data and the payments infrastructure. This is expected to stimulate the FinTech market to develop new integrated service models for both consumer and business customers.

This regulation is a reaction to the growing demand from customers as mobile and internet applications have become widely adopted driving expectations in how services should be delivered across all industries. Other market segments have adopted Open APIs to respond to this demand and have shown that innovative applications can grow business and change customer behaviour.

So far, the general response of Europe's bankers to PSD2 is one of uncertainty. Many bankers fear that PSD2 will cause them to lose control of the client interface and so remain unsure how to respond to the PSD2. As a result, they follow a defensive, wait-and-see stance that is risk averse.

In contrast, a few innovative banks, including the new digital challenger banks, along with some FinTechs have preempted the implementation of PSD2 pursuing strategies aimed at winning a leading role in the future. Progressive banks have understood that they need to shed their past and transform into digital service banks if they are to prosper in a banking environment dominated by digital savvy customers. Conversely, FinTechs have realised there are key regulatory and compliance roles which banks undertake so it is necessary to partner with them.

But none of this is without challenges for all players involved - not least from the uncertainty over finalising the last element of the regulations – the Regulatory Technical Standards (RTS). Even so there is a clear model for the operation of Open Banking and much work being undertaken to establish 'standard APIs' so banks can invest in technologies to meet their obligations and FinTechs consider offerings to be developed.

PSD2 challenges both the banking industry and the emerging FinTech sector. An irrevocable shift to Open Banking in Europe has become inevitable, and it offers both banks and FinTechs opportunities to differentiate and generate new revenues.

1.2 INTRODUCTION

The objective of this report is to analyse the implications of the revised Payment Services Directive, PSD2, for the European banking industry and Open Banking challenges both for banks and FinTechs. In short Open Banking leads to more transparency, customer choice, control over financial assets and personal data. Open APIs are a key enabler of this evolution.

With this in mind, Payments Cards and Mobile collaborated with NCR to document Open Banking trends in the payments industry. The aim is to provide insight into the level with which Open Banking, open APIs, and new FinTech and banking services can support the financial service industry' strategy to service banking customers and support service partners.

The methodology used in this report is composed of results compiled from market research both in the financial services industry, from reviewing FinTechs that are already leveraging APIs and data, and lessons learned from continuous discussions with FinTechs and financial services industry players, since 2012.

2. A UNIQUE LEGAL FRAMEWORK FOR OPEN BANKING IN EUROPE

The legal framework for payment and banking services is a joint project undertaken by the European Commission as the regulator, the European Central Bank (ECB) as the Euro System. The objective is to standardise payments in Europe and remove existing barriers, promote cross-border competition between payment services, strengthen the European internal market and drive the digital payment transformation.

Based on its vision, the EU Commission has created a unique legal framework for cashless B2C and B2B payments that supersedes pre-existing national legislation and is binding for financial service providers and payment service providers throughout the EU. As members of the European Economic Area, Liechtenstein, Norway and Iceland have largely transposed this legal framework into their national legislation.

The revised Payment Service Directive, PSD2, is the key directive for borderless banking and payment services.

Another significant regulatory trend is the implementation of the General Data Protection Regulation (GDPR) by May 2018. GDPR establishes a regulatory framework for customers' control of their data through consent mechanisms, the right to be forgotten and the right to retrieve all personal data for re-use by other service providers of choice, thereby preventing a 'lock-in' situation.

PSD2 provides the unique legal framework for Open Banking

The original Payment Service Directive (PSD) was adopted in 2007. The need to revise the PSD was due to changes in the electronic payment market such as the emergence of new types of payment services and payment service providers.

The revised Payment Services Directive, PSD2, entered into force on 13 January 2016. The EU Member States must adopt PSD2 into their legislation and national laws by 12 January 2018. The other EEA countries (i.e. Iceland, Liechtenstein and Norway) will also commit to PSD2. Switzerland has bilateral agreements with the EU and may partially transform PSD2 into its national legislation.

PSD2 introduces new services and players in the electronic payment market and extends and clarifies the scope of existing payment and banking services.

More importantly, and for the very first time in Europe, PSD2 sets the stage for pan-European Open Banking:

- PSD2 sets the mandate on Open Banking and payment services in Europe
- PSD2 grants third-party payment service providers the right of access to account data and bank infrastructure
- PSD2 regulates the open access to customer account data (XS2A) and banking infrastructure
- PSD2 mandates the rules for Strong Customer Authentication (SCA) to be provided in the Regulatory Technical Standards to be published by EBA, the European Banking Authority.

Strong customer authentication and secure communication are key to achieving the objective of the PSD2: enhancing consumer protection, promoting innovation, and improving the security of payment services across the European Union.

The European Banking Authority (EBA) is mandated to define necessary requirements for SCA and XS2A in the Regulatory Technical Standards (RTS). The EBA published its final draft of the RTS at the end of February 2017. The RTS shall apply 18 months (+1 day) after it is published in their final form by the EU Commission.

Effective from January 2018, Europe will have a unique legal framework for Open Banking, a game changer for the banking industry and emerging payment service providers – and an irrevocable shift to Open Banking in Europe is now inevitable.

Consumer Demands and Open Banking

Mobile technologies and new consumer demands have also dramatically changed the European landscape. Consumers have embraced mobile devices like tablets, smartphones, and the Internet of Things (IoT), looking for convenient ways of accessing their bank account or being able to make payments direct from the bank account. Bank customers have embraced banking apps and enhanced banking services integrated into these banking apps. As with the payments industry, security and convenience has driven consumer adoption.

The underlying trend for the 'Open Banking' concept is the increasing level of control available for bank customers on how, when, and where they use their banking services. Open Banking will allow them to access their account data at different banks through one interface either by using the mobile banking app from their bank or by using an app from a chosen third-party service provider.

3. PSD2 SCOPE AND NEW TYPES OF PAYMENT SERVICE PROVIDERS

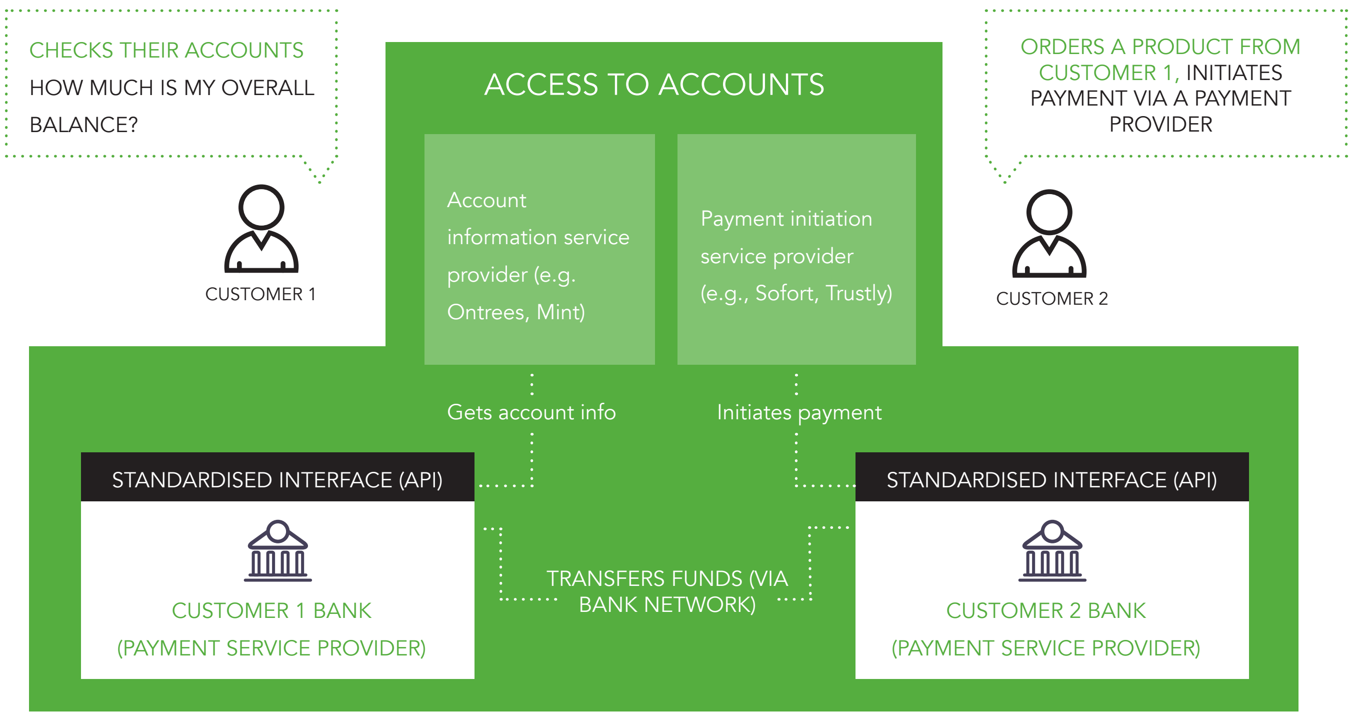
The three main topics addressed by the PSD2 cover the introduction and regulation of new parties in the electronic banking market, setting up new rules for these parties, and improving payments security.

1) The regulator intends to open the European electronic payment and banking markets for new types of payment service providers that can offer competitive, innovative payment and banking services. PSD2 regulates the role of two types of new third-party payment service providers (TPPs) and their services.

- **Payment Initiation Service Providers** (PISPs). With explicit customer permission, PISPs may initiate a payment transaction directly from the customer's bank account
- **Account Information Service Providers** (AISPs). AISPs consolidate the customer's account and transaction details from multiple accounts at multiple banks in one portal

2) PSD2 sets up the rules for access to the customer's accounts (XS2A). Banks are mandated to open their banking infrastructure to licensed TPPs. This will allow TPPs to provide account information services and enable payment initiation services. It is important to mention that these services can only be provided if the individual customer or the company serviced by the TPP has given an explicit permission for the TPP to access his account.

Figure 1: PSD2 mandates the access to accounts for data and payments



Note: The Individuals in this illustration can also be companies serviced by a TPP. Source: PCM Research.

3) Improvement of payment processing security by introduction of Regulatory Technical Standards for **Strong Customer Authentication** (SCA). SCA is an authentication process that includes two or more authentication factors. PSD2 mandates the use of SCA when the customer initiates an electronic payment transaction, whether it is to make a payment or access their bank/TPP services.

It is obvious that the RTS SCA and XS2A requirements can't be ignored even before the RTS is in place.

Notable other topics for payment services addressed by the PSD2 include:

- Transparency and information requirements for payments where only one payment service provider is in the EU ('one-leg transactions') or when paying in non-EU currency
- Inclusion of payment transactions based on a specific payment instrument within a closed payment network (for instance, a chain of department stores or a network of petrol stations under the same brand offering a dedicated payment instrument to their customers) within the PSD2 scope
- Inclusion of purchases of physical goods and services through telecom operators in the PSD2 scope
- Ban on "surcharging" for card payments, both online and in-store
- Transparency of payment fees that allow customers to know what charges, if any, are applied to payments before they are processed, including the right to view a breakdown of those charges. These charges include interchange, processing fees and other transaction related costs
- Enhancement of customer protection against fraud and capping customer liability for unauthorised payment up to €50
- Clarification of parties' liability in case of misappropriated payments initiated by TPPs
- Designation of competent authorities to handle complaints of payment service users and other interested parties

About Payment Information Service Providers (PISPs)

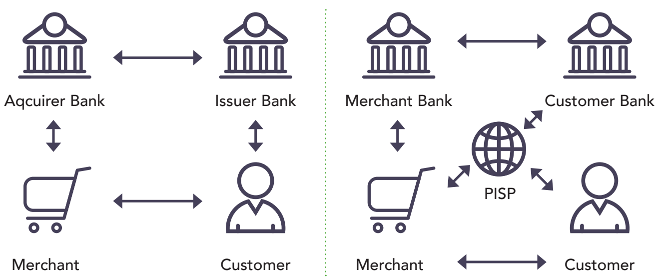
PISPs typically play an intermediate role between the customer and the merchant. PISPs establish a gateway between the merchant's website and the online banking platform of the customer's bank. They offer IBAN-based credit transfers, and/or direct debits, and/or other online payment solution alternatives to card payments.

Before PSD2, customers typically paid for online purchase using a card. The merchant's card acquirer would then execute the payment (via a card scheme) debiting the customer's bank account (Figure 2 – left).

In the post PSD2 world, the customer may be asked whether they would give the PISP explicit permission to initiate a payment from their bank account. Without giving their bank login details to the PISP, the customer would give explicit permission to the PISP to execute payments on their behalf from their bank account (Figure 2 – right).

PISPs claim to enable easier and cheaper payment services for individuals and companies with immediate notification to the merchant about payment initiation. Figure 2 shows how PISPs may change four-party payment models. A key difference to the four-party model is that payment credentials are no longer stored on merchant systems.

Figure 2: The role of PISPs – Illustrative

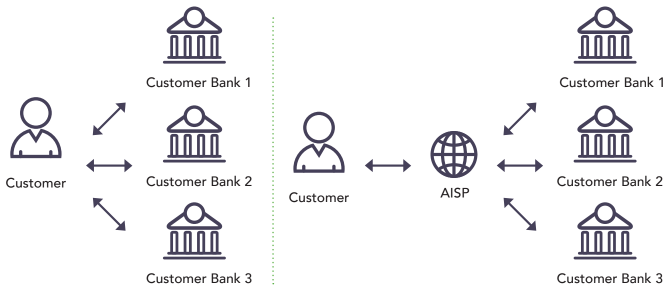


Note: Customers can be individuals and companies serviced by PISPs. Source PCM research.

About Account Information Service Providers (AISPs)

AISPs are intended to allow customers to have a 360 degree view of their payment account data. For instance, AISPs can provide a single online portal to consolidate different payment accounts the customer may have with one or more banks and categorise the payment history. In this case, the customer does not need to log in separately to each bank's online platform. The customer accesses all their account information via the AISP without giving the actual bank login details to the AISP (Figure 3 – right. Figure 3 compares the current mechanism with the AISP mechanism).

Figure 3: The role of AISPs – illustrative



Note: Customers can be individuals and companies serviced by AISPs. Source PCM research.

Limited Information Exchange under XS2A Mandate

PSD2 mandates that the sensitive data exchanged between TPPs and banks is as minimal as possible, e.g. a TPP may only receive a Yes/No answer from the consumer's bank about availability of funds before initiating the payment.

However, PSD2 does not specify the exact definition of customer sensitive data and does not provide requirements on the information that TPPs can have access to. It is expected that the EBA will provide more guidance on using and exchanging sensitive customer information in the final RTS document to be published.

Therefore, TPPs may focus on the following types of services as envisioned in Figure 4.

Figure 4: XS2A information exchange between FinTechs and banks – illustrative

Service	Input data proivided by TPP to bank	Bank response given to TPP
Payment initiation	IBAN from, IBAN to, Amount, TPP ID/Certificate, Authentication method?	Confirmation of payment initiation & timestamp or error code
Sufficient funds	IBAN, amount, time, TPP ID/ Certificate	Yes/No response, timestamp
Balance Information	IBAN, Filter parameters (period, IBAN to, amount) TPP ID/ Certificate, Authentication method?	Balance, payment statements
Account verification	IBAN, TPP ID/ Certificate, Authentication method?	Yes/No response (account exists, account valid)
Identity information	ID information (age, postal code, mobile number etc)	Yes/No (for example for age verification)

Source PCM research.

4. IMPACT OF PSD2 ON THE BANKING INDUSTRY AND FINTECHS

The adoption of the revised Payment Services Directive, PSD2, has set the stage for Open Banking in Europe. The European Open Banking Mandate is expected to have a significant impact on both the financial services industry and new third-party providers (TPP).

One reason is that it lowers the barriers for market entry to third-party service providers and FinTech companies. It opens up doors for innovative players in the payments and banking markets that offer services that currently do not exist, e.g. account information services, digital identity, Know Your Customer services (KYC).

In addition, PSD2 is viewed as a driver for new technologies and services. Its challenges for banks and FinTechs include Open Banking, Open APIs, and the rollout of digital payment services and mobile banking apps.

As all payment service providers are regulated by PSD2, they benefit from the unique legal framework for Open Banking and payment services. Therefore, PSD2 stimulates the development of a wide range of new banking services and new business models. However, banks and FinTechs need to amend or enhance their existing business models.

The PSD2 is going to change the European payment and banking landscape and ultimately the position and the role of banks in the ecosystem. FinTechs are set to help drive this change with the banking industry. Ultimately, both parties are seeking the right strategy for success.

Post-PSD2, the key question for the financial service industry will be how to grant authorised access to their FinTech partners for bank account information e. g. account balance, payment data, credit risk and others.

In other words: What do banks need to offer in terms of support to FinTech partners, e.g. access to bank systems through a set of their own Open APIs?

Impact of PSD2 on FinTechs

Like digital challenger banks in Europe, most FinTechs already have a clear Open Banking strategy in place.

They already compete with the banks and demand standardised Open APIs to get authorised access to customer account data and banking infrastructure. From the FinTech point of view, Open APIs are a pre-requisite to provide their Open Banking services to consumers and bank clients.

FinTechs threaten not only to capture a piece of the banks' revenue, but also to disrupt the complete banking sector. For them, PSD2 defines the rules to access the customer's accounts (XS2A) by mandating banks to open their APIs to third-party providers (TPPs).

FinTechs understand that PSD2 creates the framework for the legal rollout of new payment and banking services. Although the fragmentation of multi-channels and the complexity of connecting to proprietary banking infrastructure might be an initial hurdle to achieve transaction volumes.

Selected business and service challenges for FinTechs include:

- All third-party providers (TPPs) need to register with the financial authorities to get licensed according to the PSD2
- AISP strategy for access to account information offerings: compete/partner with banks
- PISP strategy for IBAN-based payment service offerings: compete/partner with banks
- Combined mobile apps: payment services, account information, value-added convenience services
- Use of bridging technologies to enable payments in-store, in-app, online and e-billing: NFC / QR / Bluetooth Low Energy (BLE)
- Compliance with security standards: Tokenisation, RTS SCA: e.g. Mobile Transaction Authentication Number (mTAN)

- Implement access to bank accounts and bank infrastructure based on Open APIs or on multiple proprietary APIs
- Complexity: The range of APIs to be implemented. There is no common Open API standard in place
- Enhanced business strategy: Partner agreements with banks and/or other FinTechs

Although PSD2 mandates the access to bank accounts and bank infrastructure based on APIs, the greatest challenge for FinTechs is how to get access to bank infrastructure bank by bank.

Key questions for FinTechs include:

- Which banks to partner with for authorised access to bank account information?
- Which account information details will be available (e.g. account balance or just Y/N)?
- What API support services will be offered by banks: individual APIs versus Open APIs?
- Which banks already offer a set of Open APIs to connect to its infrastructure?
- What partner agreements for XS2A information exchange services are offered by banks?
- XS2A implementation process with a bank: technical approval/certification/E2E-security?
- XS2A service cost for setup/processing/services invoiced by banks?
- Are there third-party XS2A network processors which can connect to multiple banks?

According to key FinTech players, they expect the banks to offer support in terms of Open API interface and supporting services during set-up and appropriate processing service levels for XS2A information exchange.

Impact on the Banking Industry

PSD2 will allow bank customers to decide who they want to grant access to their payment information, meaning a disconnect between banks and the direct connection to their customers. To maintain their position in the new PSD2 reality, banks will need to adapt their business and operational models.

For example, banks will have to decide on a new Open Banking strategy in line with GDPR and PSD2 regarding:

- Connect its own apps and third-party apps directly to a bank account?
- Connect bank account data to its own apps and to third-party apps?
- Login at third-party websites with existing banking credentials: e.g. login, identification, authentication?
- After authorisation with existing banking credentials, do they share personal client attributes with third party websites: e.g. name, age, email address?

So far, the overall response of Europe's bankers to PSD2 is one of uncertainty. Although many bankers fear that PSD2 will cause them to lose control of the client interface, many of them remain unsure how to respond to the Open Banking mandate of the PSD2. As a result, most banks have followed a defensive, wait-and-see stance that is risk averse.

In contrast to the majority of European banks, a few innovative, digital challenger banks have not waited until the implementation of PSD2 in each EU Member State. They have embraced the possibilities of Open Banking, Open APIs, and pursue strategies aimed at winning a leading role in the future.

Innovative banks that embrace Open Banking have provided use cases and offer their own sets of Shared API interfaces. These banks understand a clear strategy to support new banking service partners. Some banks have understood that they need to shed their past and transform into digital service banks if they are to prosper in a banking environment dominated by technologically astute consumers.

According to the 2016 European Survey by PWC Strategy, European banks executives revealed a mixed, but mostly negative PSD2 perception, unclear regarding their own position in the Open Banking world:

- 88% expect PSD2 to have an impact on their business
- 84% expect strategy changes due to PSD2
- 68% feel they will be weakened as a result of PSD2
- 68% are concerned about losing control of their customer interface
- 52% think there will be a risk of liability problems

However, 44% of the interviewed banks said they plan to provide an Open Bank offering in the next five years:

- 64% intend to integrate third-party products or services into own digital offering
- 44% plan to integrate own products or services into third-party ecosystems
- 32% expect to offer new services and functions that are essential for existing ecosystems

Selected business and service challenges for the banking industry include:

- Allow FinTechs access to bank accounts and bank infrastructure by publishing their own set of shared APIs
- Own service strategy: in-app use of card-less payment services versus card payments
- Compete/partner with AISPs: strategy for granting access to account information to AISPs
- Compete/partner with PISPs: strategy for IBAN-based payment services initiated by PISPs
- Combined mobile apps: payment services, account information, value-added convenience services
- Use of bridging technologies to enable payments in-store, in-app online and e-billing: NFC/QR/BLE
- Compliance with security standards: Tokenisation, RTS SCA: e.g. mTAN
- Enhanced business strategy and service support: Partner agreements with selected FinTechs in order to use them as part of the bank's own services
- New Strategy: Transformation to be a digital banking hub consolidating other banks and FinTechs

Although PSD2 mandates the access to bank accounts and bank infrastructure, the greatest challenge for banks is how to grant access to their infrastructure, FinTech by FinTech. **Key questions for banks include:**

- Decision to offer partner agreements: Which FinTech partners to select for enhancing the bank's own services?
- Which account information details should be available (e.g. account balance or just Y/N)?
- What API support services will be offered: individual bank specific APIs versus Open APIs?
- XS2A implementation process with FinTechs: technical approval/API testing/certification/E2E-security?
- Decision to invoice FinTechs for XS2A service cost for setup/processing/support services?
- Decision to connect to third-party XS2A network processors which can connect to multiple FinTechs?

Generating Value in an Open Banking ecosystem

According to FinTechs and first mover banks, they are aware of new opportunities to generate value from services in a decentralised, future Open Banking ecosystem where the correct business strategies are implemented (Figure 5).

Figure 5: Business Models to generate value from Open Banking services

	Strategic rationale	Value generation
1. Third-party module sourcing	- 'Defend' customer interface by being innovation leader in products and services - Support own innovations, reduce time-to-market through external sourcing via API's in a fast, cost-effective, flexible way	Lower development costs, customer engagement and retention
2. Third-party data sourcing	- 'Defend' customer interface by better understanding customers and developing data-driven, customer-centric products and services	Customer engagement and retention
3. Banking module provider	- Expand banking to new use cases by enabling partners to integrate bank modules in own offering - Support innovation through collaboration with external partners	Customer acquisition, cross-selling, and new businesss (API partners)
4. Banking data provider	- Build up new business of providing high-class/premium data to third parties	New business (API partners)
5. Digital platform	- Become a true innovation leader, providing the best products and services by establishing a 'mutual relationship' with third parties	Potentially all of the above

Source: Information compiled from discussions with banks and FinTechs, PCM research

5. ABOUT OPEN APIs

For many years, Application Programming Interfaces (APIs) have been commonly used for sharing data and interconnecting platform solutions with Third-Party Providers (TPPs). Large companies such as Google, Twitter, Facebook, and Uber offer APIs to third parties to login or to initiate messages, for example.

APIs come in many shapes and forms, varying from private (internal within one organisation), to partner (between organisations) and public ("open") versions. In all instances, APIs come with technical specifications, testing facilities and clarity under which legal and operational conditions the APIs can be used. 'Open APIs' are APIs, which are open to third parties to digitally connect services.

By introducing the Open API concept for Open Banking ecosystems, the PSD2 sets up new rules for accessing bank accounts for TPP players (XS2A). PSD2 mandates all banks to allow TPPs to be able to access customer account information and payment initiation services if, and only if, the customer has explicitly granted permission to the TPP to initiate such requests and that the TPP is registered by the competent financial authority of its home country.

Subject to adoption of the EBA RTS, Open APIs could be an effective and automated means to enable appropriately licensed TPPs to connect to payment accounts in a secure manner, i.e. without compromising security standards and minimising exposure of sensitive payment and account data.

The API concept of Open Banking sounds promising, but it is also a big challenge from a security perspective. PSD2 mandates TPPs to authenticate themselves towards banks and communicate securely with the bank, the payer and the payee. Financially sensitive transaction data must be securely exchanged and must not be accessible by any other party than the bank and the TPP, the latter having the explicit permission of the bank customer.

From an industry perspective, Open Banking challenges include the need for proper standardisation of APIs (beyond pure technical dimensions) and collective customer education on new possibilities and secure behaviour when they are exercising control over financial assets and personal data in relation to third parties.

Innovative banks are working at the forefront of Open APIs. Based on a clear Open Banking Strategy, they prepare the launch of their own sets of API interfaces and are prepared to partner with TPPs. By mid-2017, more than 50 European and worldwide banks say they are doing this, including:

Source: The Paypers.

Example – BBVA launches its Open API market place

In May 2017, BBVA said it is making eight of its own APIs commercially available to companies, start-ups, and developers worldwide, enabling the integration of customer banking data with third party products and services.

The launch of the BBVA API Marketplace comes after the Spanish bank spent more than a year working with developers and businesses to fine-tune the way the Open API services would be delivered. During this time, over 1,500 businesses and developers registered with the experimental portal in Spain.

Initially only Spanish customers of BBVA will be able to benefit from the marketplace - but the bank intends to roll-out the programme to its US customers later this year, before expanding it further to include Turkey, Mexico, Latin America, and beyond.

BBVA said it is already working with 35 Spanish companies, but also with geo-marketing start-ups such as Geoblink, Carto or Bismart, and with software vendors, such as Anfix, Simplygest, and Sage.

Example – Berlin Group to publish single API standard for PSD2

In June 2017, Berlin Group, the European payments interoperability coalition of banks and payment processors, announced a single standard for API access to bank accounts to comply with new PSD2 regulation regarding XS2A.

The Berlin Group says its NextGenPSD2 Initiative will help overcome the emergence of multiple competing mechanisms in the market by providing a harmonised API standard for accessing bank accounts.

The Group carries some heft in European markets, with membership comprising bank-backed ACHs and industry bodies across the length and breadth of Europe.

Built as an ‘Access to Account Framework’, the Berlin Group says the standard will offer operational rules and implementation guidelines with detailed data definitions, message modelling and information flows based on RESTful API methodology. It will be published for consultation in Q4 2017.

6. ABOUT OPEN BANKING USE CASES

As a technology driven evolution, Open Banking impacts both retail and corporate bank client segments and service domains spanning payments, cash management, lending, savings, wealth management, mortgages, and other value-added services.

Assessing the early mover banks and start-up players with focused business models, emerging Open Banking trends in Europe include combining banking apps with payment services and value-added convenience services from TPPs for clients. Among others, Open Banking services operated by FinTechs and early mover banks in Europe include:

- Barclays banking app 'Pingit' - for bill payments and P2P transfers
- Klarna's Sofort – online credit transfer payment service to pay for online purchases
- SlimPay – online direct debit payment service to pay for online purchases
- BlueCode – 1D-barcode initiated direct debit payment service to pay for outlet purchases
- MyUros – PFM app connecting to multiple payment accounts at different banks
- Smart Fridge – authorisation of a smart fridge app for recurring automatic order and payment of groceries up to €50
- JITFinTech – requesting personal loan by one-time sharing account data
- FinanceApp – cash flow prediction and financial advice based on account data

As a result of discussions with key players, the Open Banking use cases identified in European markets are composed of banking services, payment services, personal finance management services (PFM) and complementary value-added services. For illustrative reasons, selected use cases for individuals are listed here:

1) BY BANKING SERVICE TYPES

- Branch locator
- ATM locator
- Bank products/service information
- Digital personal assistant (a kind of bank's Alexa)
- Overview of all the bank accounts and wallets
- Manage accounts, cards, wallets, digital payment means, saving accounts
- Checking the actual account balances
- Consumer Finance, revolving credit, personal loans, car purchase finance …
- Buying or selling stocks

2) BY PAYMENT SERVICE TYPES

- Online banking: credit transfers, direct debits, immediate payments
- Recurring payments and e-Mandate management
- Mobile money transfer, e.g. P2P, mobile remittance
- In-app payments at any place: POS/mPOS, online, QR-initiated, HCE NFC in-store
- Card-less cash withdrawals at ATMs or cashback locations

3) BY THIRD-PARTY PROVIDER SERVICE TYPES

- Receiving messages across banks
- Information search across banks
- Recurring payment management for subscriptions
- E-Billing and e-invoicing management across banks
- Revolving credit, Instalments
- Personal financial management
- Requesting personal loan at lender sharing selected account data
- Cash flow prediction based on account data across banks
- Financial advice and possible actions based on account data across banks

- Automatic order and purchase through TPP app used
- Loyalty, bonus points, benefits for app services used
- Special events and tourist attractions offered by TPPs partnering with banks or other TPPs
- Discounts at merchants offered by TPPs partnering with the banks or other TPPs

From the perspective of the individual consumer or company, there are three key choices to find a partner for an API-based set of combined Open Banking use cases:

- Select a bank and the TPP partners connected with this bank. A bank centric approach, e.g. a digital challenger bank, a large European banking group
- Select a FinTech servicing across banks and the TPP partners connected with this TPP. A kind of Uber-like approach: one TPP acts as financial services hub covering other banks/TPPs to meet the service scope
- Use a mix of banks and TPPs in order to achieve the service scope

In order to illustrate the process of API-based Open Banking use cases, three examples are illustrated (see below). Generally, all use cases require, as a first step, the customer's explicit permission to the TPP to process the use case, either one-time or recurring. In a second step, the TPP completes the use case demanded, for instance making a payment request.

The most important lessons learned while talking to FinTechs and financial services industry players is that any combination of Open Banking use cases is technically possible.

In a few years from now, banking apps on mobiles and tablets are expected to combine account management, payment services, account information, personal finance management, and value-added convenience services.

Example 1 – card-less payment initiation workflow using a FinTech app

Use Case: Customer buys online and wants to pay the merchant card-less direct from his bank account. The PISP provides payment initiation services, has API-based access to the customer's bank and pays the merchant.

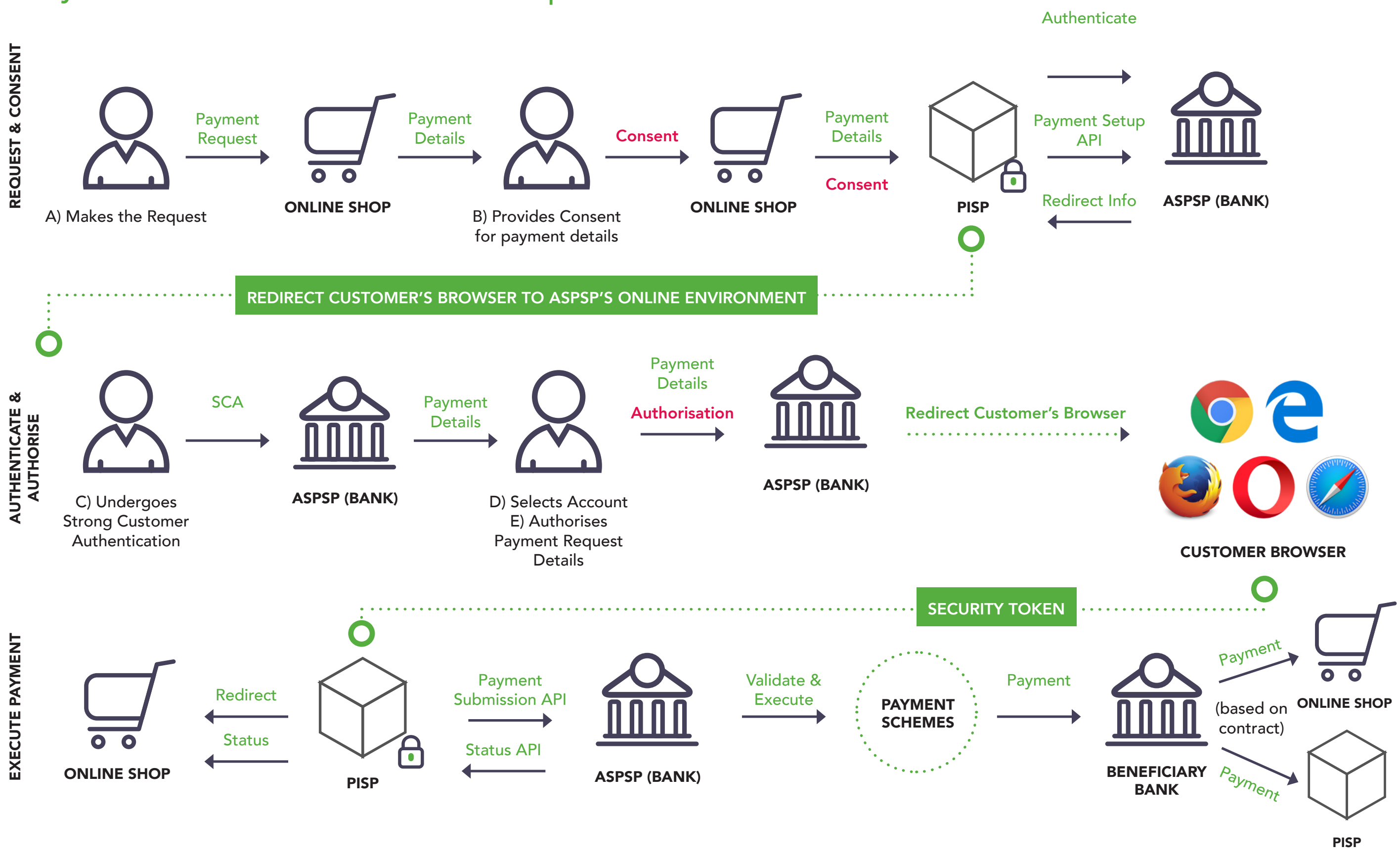
Step 1: Giving explicit one-time permission to PISP to initiate a payment on behalf of the customer:

1. Customer clicks the PISP button on the payment page of the online shop in order to request a payment. The merchant provides the consent payment details to the PISP
2. Customer selects 'Pay from bank account' on the PISP payment page, e.g. credit transfer or direct debit
3. PISP redirects the customer to their bank. Customer logs in to their bank (undergoing a SCA)
4. Customer authorises the bank to grant the one-time permission to PISP for executing the payment on their behalf based on the pre-filled payment details
5. Customer's bank returns to the PISP a token confirming the rights to funds for this payment

Step 2: Payment execution processed by PISP:

6. PISP completes the shopping process and performs the SCA process on behalf of the customer. Here, the PISP may perform the customer authentication using its own mechanism or may choose to use the customer's bank authentication method (e. g. one-time TAN code to customer's smartphone)
7. PISP uses the API to present to the bank the request for payment along with the token provided in step 5. The bank validates the token matches the request from the PISP
8. Customer's bank initiates the transfer of funds directly from the customer's account and credits the merchant.

Payment Initiation API Flow for Example 1



Example 2 – Access to multiple-bank account statements using FinTech app

Use Case: Customer uses one FinTech app to monitor all bank accounts at different banks. The AISP provides account information services and has API-based access to all the customer's banks.

Step 1: Giving explicit permission to AISP to periodically collect account data on behalf of the customer:

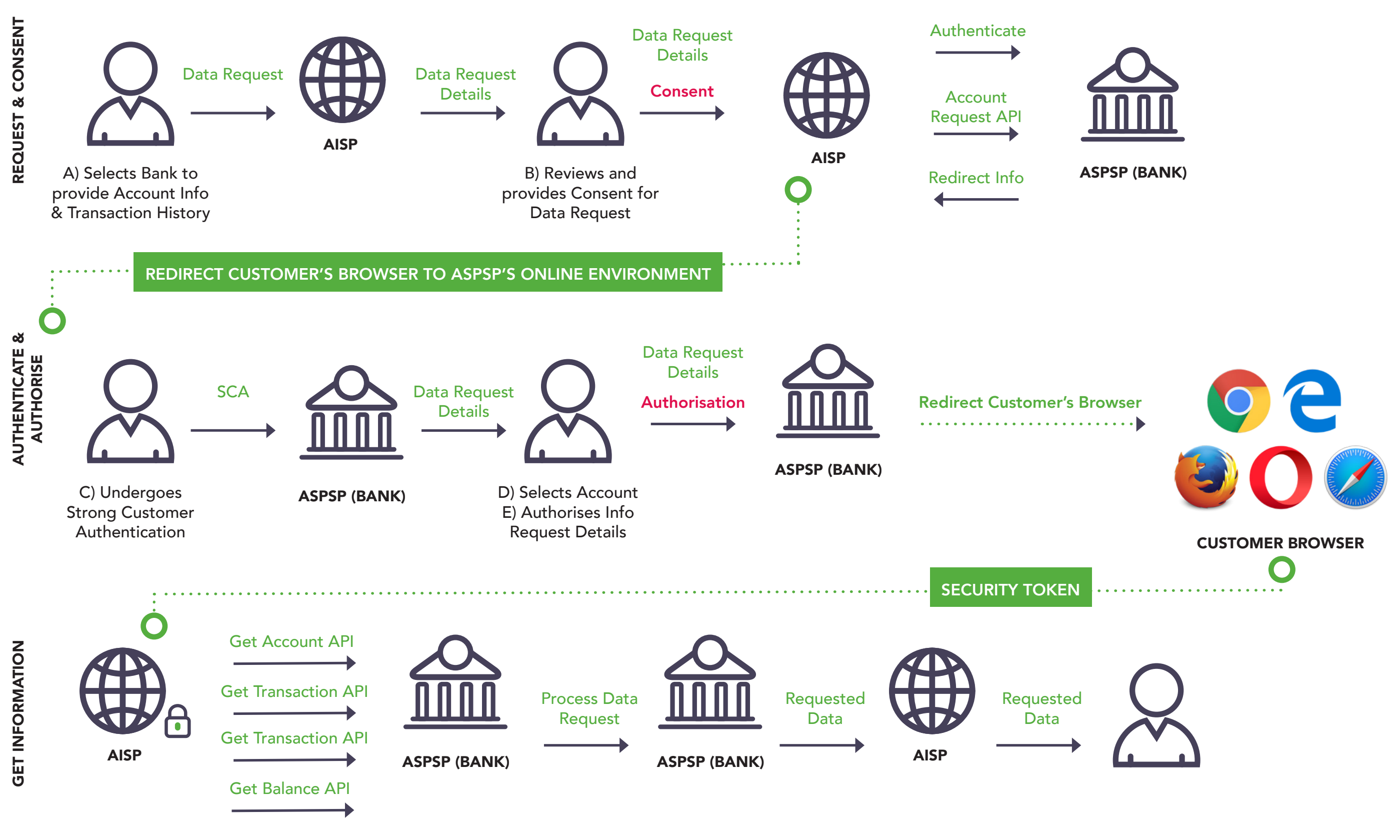
1. One-time Initiation: Customer connects all selected bank accounts bank by bank to the AISP app
2. For each account and bank-by-bank, AISP redirects the customer to the bank to grant the explicit recurring permission for the AISP to collect consented account data on behalf of the customer
3. For each account and bank-by-bank, customer logs on to the bank (undergoing a SCA) and confirms the account linking via the banks' authentication credentials (e.g. electronic ID)
4. Here, the customer authorises each bank to provide bank statements to the AISP, e.g. three months for the respective bank accounts
5. Each bank provides a token to the AISP incorporating the entitlement to access the account data linked to the AISP. Customer has linked multiple accounts at different banks within the AISP app

Periodic Step 2: Update of bank account statements by AISP on behalf of the customer:

6. Periodically, the customer clicks the AISP app and chooses to see bank account balances and bank statements
7. Bank by bank, the AISP uses the API to request the account data from the bank along with the respective token provided in step 5. Each bank validates the respective token matches the request from the AISP
8. AISP performs a Strong Customer Authentication process on behalf of the customer. AISP may perform the customer authentication using its own mechanism or may choose to use the customer's bank authentication method (e. g. one-time TAN code to customer's smartphone)
9. Bank-by-bank, AISP retrieves the actual bank statements of the bank accounts connected to the AISP app
10. Customer has the transactions overview from multiple bank accounts connected to the AISP app

Additional Service Option: Customer can initiate payments from linked accounts through the AISP app, in the case that the AISP also acts as a PISP or is connected to the customer's preferred PISP. In this instance another set of explicit permissions would be required as outlined in Example 1.

Account Information API Flow for Example 2



Example 3 – Convenient predictions and financial advice using FinTech app

Use Case: Customer uses one Fintech app to get financial advice based on all of his bank accounts at different banks. The AISP provides financial advice and has API-based access to all of the customer's banks.

Step 1: Giving explicit permission to AISP to periodically collect bank account data on behalf of the customer

A set of explicit permissions would be required as outlined in example 2.

Periodic Step 2: Update of bank account statements by AISP on behalf of the customer

The periodic update of bank account statements would be required as outlined in example 2.

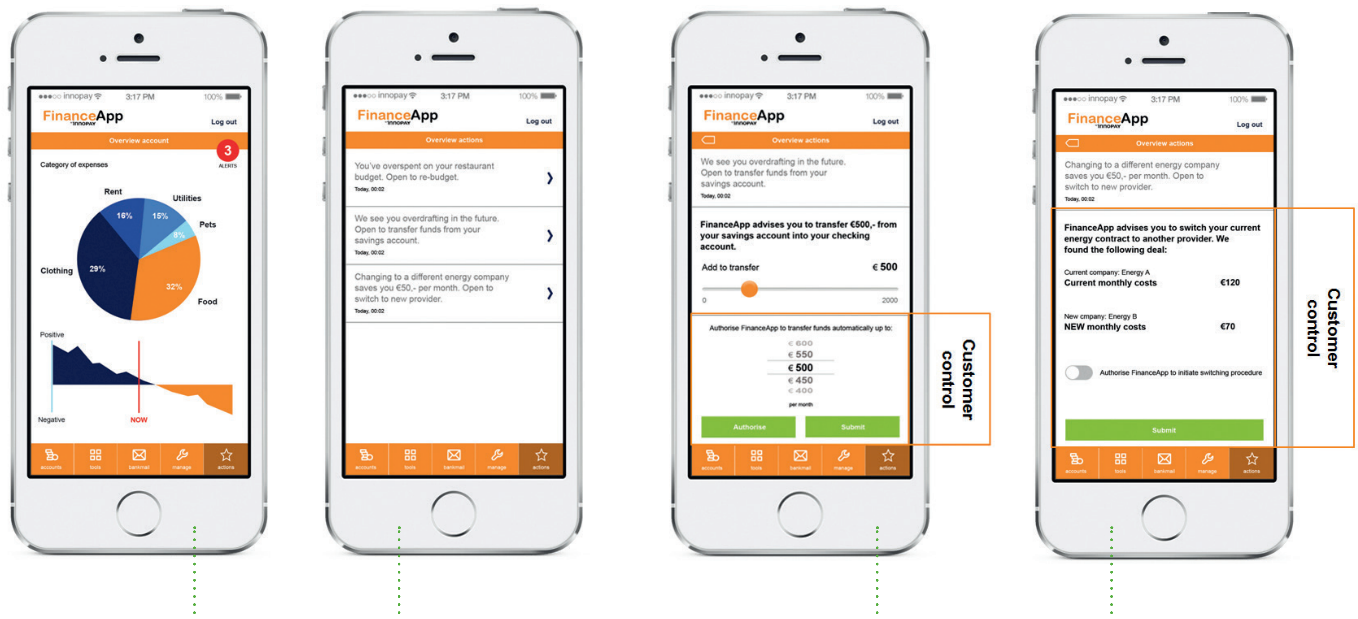
Step 3: cash flow prediction and financial advice by AISP based on retrieved account data

1. AISP provides convenient predictions, financial advice, and may propose potential actions to the customer. That could extend to actually moving money between accounts (perhaps from a current account to a savings account) which would be a payment request carried out with another set of explicit permissions as outlined in example 1. In this case the AISP is also acting as a PISP.

2. In addition, AISP app may provide suggestions for best offers based on benchmarking, e.g. consumer loans. Again these could extend to actually taking up the proposed service in which case specific permissions may be needed to gather additional data or to make a payment with the AISP acting as a PISP.

Additional Service Option: Customer can initiate payments from linked accounts through the AISP app, in the case that the AISP also acts as a PISP or is connected to the customer's preferred PISP. In this instance another set of explicit permissions would be required. Then the customer can authorise payments through existing bank credentials (see example 1 above). In this case the customer can automate such payments in the future using the AISP app and/or PISP app.

Illustrated Consumer View for Example 3



CUSTOMER SEES PREDICTED CASH FLOW BASED ON ACCOUNT DATA

FINANCE APP PROVIDES FINANCIAL ADVICE AND PRESENTS POSSIBLE ACTIONS TO THE CUSTOMER

FINANCE APP ALSO ENABLES USER TO INITIATE A PAYMENT AND TO AUTOMATE SUCH TRANSFERS IN THE FUTURE

FINANCE APP PROVIDES USERS WITH SUGGESTIONS FOR BEST OFFERS BASED ON BENCHMARKING

Source: EBA Open Banking Working Group: Open Banking – advancing customer-centricity / analysis and overview

7. ABOUT OPEN BANKING PLATFORMS AND BUSINESS MODELS

The payments industry is well known for its mature ecosystems and has diversified into decentralised service models like issuers, acquirers, payment processors, PSPs. The same can be identified in the Open Banking ecosystems.

In parallel to the in-house Open Banking platforms of innovative banks (e. g. Spanish BBVA Group), diversified Open Banking platforms open for partnerships with TPPs have emerged. They create API-powered, customer centric, data driven business models.

Assessing early movers in Europe, new business model providers can be identified, including Buddybank, Figo, N26, Open Bank Project, Satispay, Treefin and Clearbank. Ever since its inception in 2016, the PSD2 has encouraged new types of business models (see Figure 7):

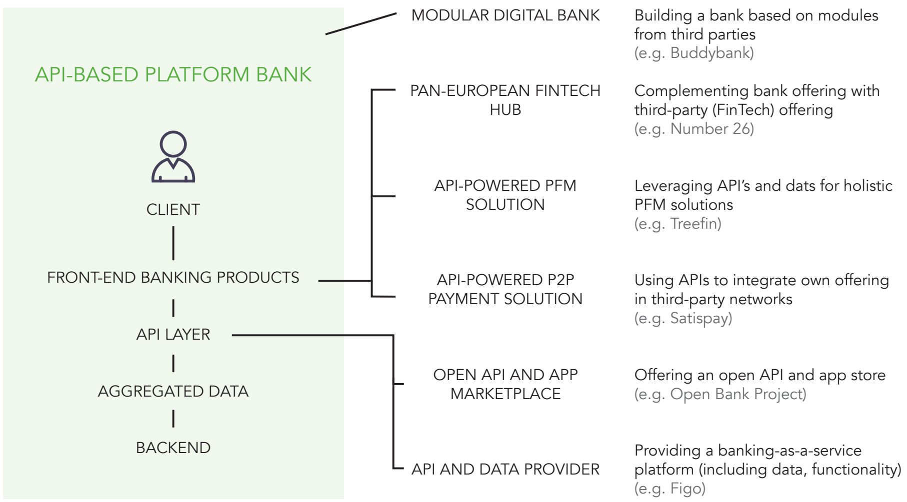
- Modular digital bank – Building an Open Bank platform based on services from third parties (TPPs)
- Digital mobile bank acting as financial services hub, competing with traditional bank
- Personal financial management app service model integrating multiple banks and FinTechs
- Payment service app solution providers integrating their own offering in third-party networks (bank, retailer, telco)
- White-label Open app and API marketplace
- Cross-Banking platform and API solution management as a Service (SaaS model)
- Cross-channel transaction network service processing solutions for payments and Open Banking connecting banking apps, payment service providers, and FinTechs with banks

According to market players, the user experience of Open Banking platforms is strongly influenced by the digital identity user experience, via mobile, SMS or one-time codes (e.g. a transaction authentication number).

From a bank point of view, Open Banking platforms will include four generic service roles: integrator, producer, distributor, and platform. They may be supported by four API-based layers (see Figure 6):

- Front-end for banking products – own and TPP products
- API layer – open for connecting with selected TPPs
- Aggregated data layer – in-house
- Back-end banking systems – in-house

Figure 6: API-based Open Banking platform scenario models – illustrative



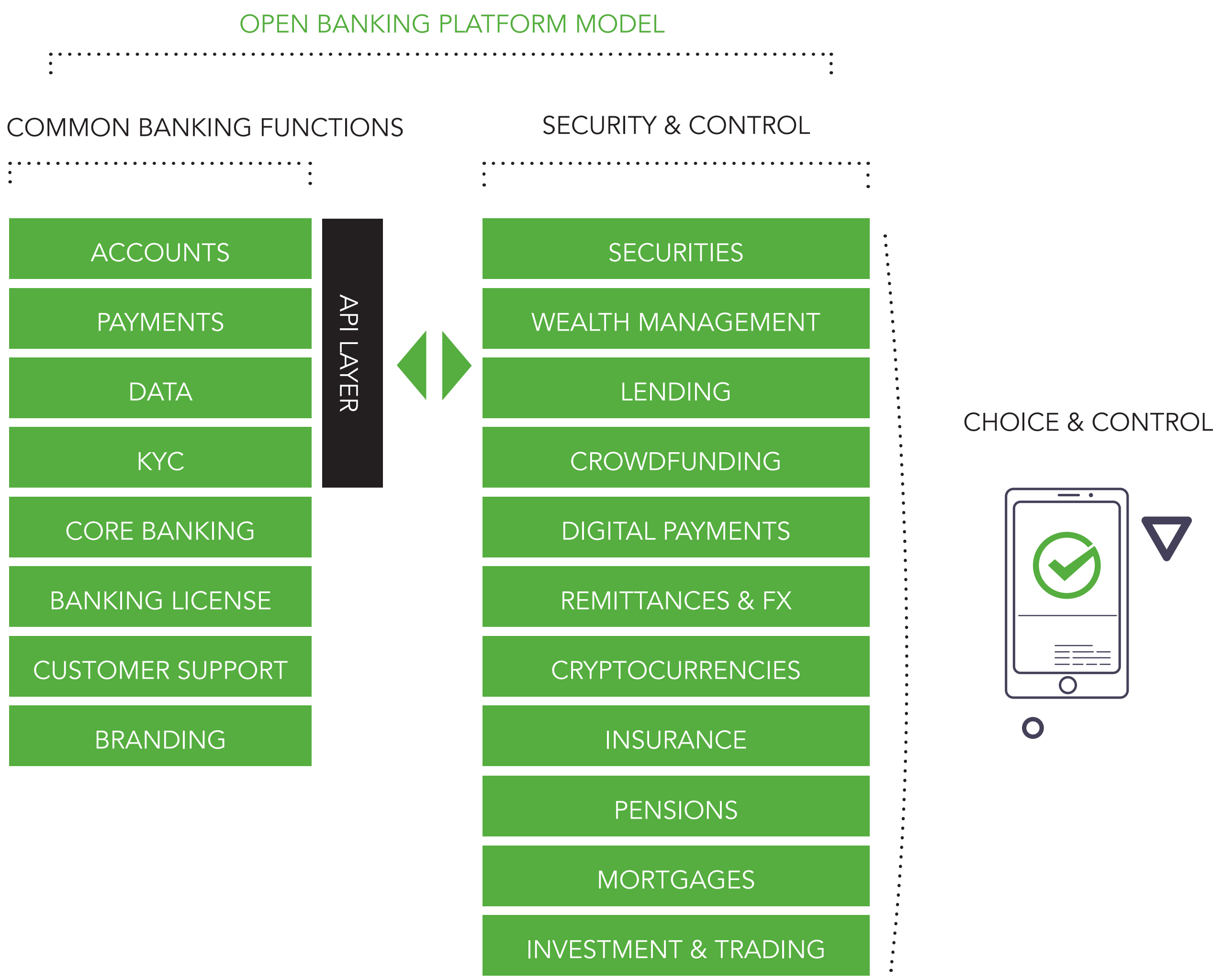
Source: PCM Research

According to the European Banking Association, seen from a customer perspective, API-based Open Banking platform models are based on the following service layers (see Figure 7):

- Mobile App Layer: Bank Customer Choice and Control
- Security and Control Layer: managing the Open Banking use cases
- Common Banking Functions – defined as existing core banking systems and/or processing partners

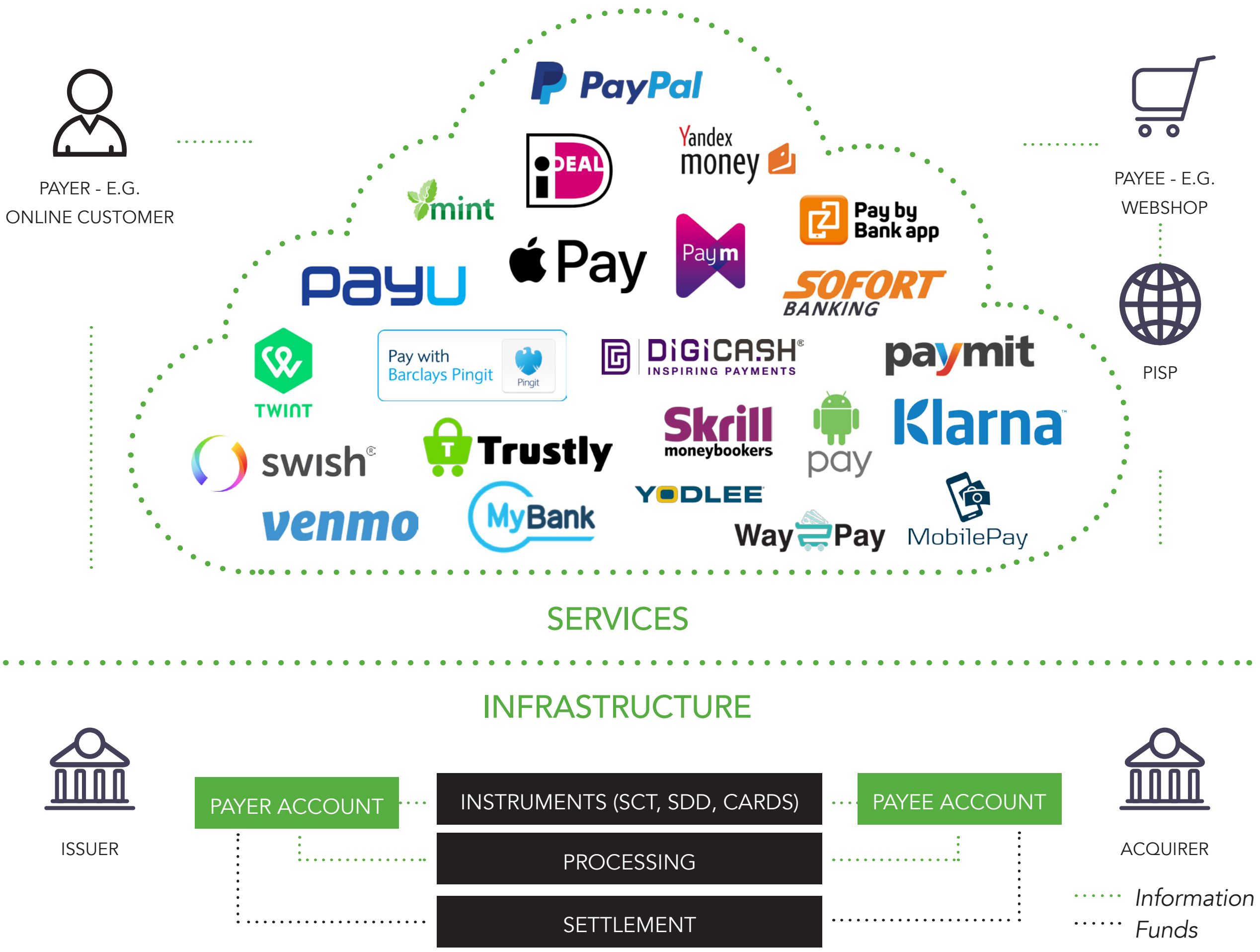
For the payments industry, a specific payment layer on top of the banking infrastructure is already de facto practiced in Europe. Figure 8 illustrates the API-based platform model with a service layer for FinTechs and the banks' payment infrastructure. It is obvious, that payment complexity for merchants and consumers is part of the below model.

Figure 7: Open Banking Platform Model



Source: EBA Open Banking Working Group: Open Banking – advancing customer-centricity / analysis and overview

Figure 8: The payment services layer on top of the bank payment infrastructure layer



Source: EBA Open Banking Working Group: Open Banking – advancing customer-centricity / analysis and overview

8. CONCLUSIONS

The adoption of the revised Directive on Payment Services (PSD2) has set the stage for Open Banking in Europe – a European Open Banking Mandate – providing open access to customer account data and payments infrastructure.

Despite the clear framework for the future European electronic payment and banking market and an implementation date of January 2018, there are important elements of the regulations that have been delegated to Regulatory Technical Standards which are yet to be confirmed leading to a 'fuzzy' period where the rules seem unclear.

Whatever the timescales, PSD2 requires banks and third party processors (TPPs who are typically FinTechs) to change their relationships, with each required to adapt to the PSD2 mandate.

That requires banks to:

- Evaluate their strategy and the impact of PSD2, especially the digital relationship with their customers
- Decide whether to make use of one of the shared APIs or launch their own
- Implement the APIs including orchestration of the new transaction processes allowing flexibility to adjust to the requirements of the RTS as it comes into force
- Consider becoming a Third-Party Processor (TPP) and providing new services and business models to customers (consumers and businesses) potentially through collaboration with FinTechs

Equally fintechs have some decisions to make:

- Consider the impact on their current business models especially the registration requirements
- Change their technology to use the APIs with the expectation of needing further change as banks implement the full requirements of the RTS
- Identify new services that can be offered to customers (consumers and businesses) perhaps through new collaborations

For banks, there is a danger of being left behind while losing the direct customer relationship. They specifically will have to implement new technical interfaces and possibly change their online authentication approach. Acting quickly is crucial for the bank to secure their position in the future European Open Banking ecosystem.

For the FinTechs, the potential business opportunity from the opening of banking APIs cannot be underestimated.

As with any shake up in the banking landscape the ultimate outcome is unclear. Certainly, more innovative payment and banking services will be offered in Europe by local and international service providers supporting the demand for more digital services. And, over time, direct payment from a bank account will become one of the standard offerings in many retailer e-commerce sites. However, whether it leads to banks losing their direct relationship with the customers is uncertain and unlikely, in the short to medium term, given the inertia to change exhibited in the majority of customers.

9. ABOUT THE RESEARCH

Payments Cards & Mobile

In business since 1994, Payments Cards & Mobile is an established hub for global payments news, research and consulting. We work with recognised industry experts to provide impartial, up-to-date and relevant information and analysis on every area of payments.

Personal relationships have been the hallmark of our business. We remain committed to working closely with our many long-standing customers and welcome new customers in producing quality business intelligence and providing a variety of ways in which you can consume this information. Our aim is to provide you with the highest quality data so you can position your business and key personalities in this increasingly competitive industry.

PCM Research

Payments Cards and Mobile Research offers comprehensive, in-depth research into topics which are relevant and tailored to our clients' needs.

Our in-house research facility is available for short term projects. We specialise in M&A activity, market entry data, country report analysis and statistics. Research reports on banking, payments and mobile payments worldwide.

Topics range across the measurement of efficiency and performance, card and payment service related information, the role of brands in banking and the impact of non-banks such as retailers and FinTechs on the financial services and mobile financial services market.

Payments Cards and Mobile offers specific research on all aspects of banking, card payments, card-less digital payments, Issuing/Acquiring, financial services and the mobile financial services market.

NCR

NCR is a leading provider of solutions for the financial industry including banks, FinTechs, processors, issuers and acquirers, ISOs as well as merchants. NCR's portfolio includes software products for processing payment transactions and enterprise fraud detection across many channels including ATM, POS, branch, internet banking. These products are designed to allow customers to easily adapt to the changing demands of the payments landscape whatever direction PSD2 takes you.

Acknowledgements

The report draws on publicly available information, the PSD2, EBA documents and on comments both from FinTechs and from financial services players. The author thanks EBA and various financial service organisations for the information and insight provided and the helpful responses to selected questions on Open Banking, Open APIs and digital banking services.

Author

Since 2011, Horst Forster is co-editor of the European Payment Cards Yearbook, responsible for market analysis and for compiling/writing the country profiles. Horst has expertise in both the card business and card-less digital payment services since 1996. Cross business and cross borders – his profession is business development and market intelligence services for the Payments Industry. In addition, he focusses on digital payment strategies and transformation.

Copyright

Disclaimer

While every effort has been made to ensure the accuracy of all data and information in this report, it is provided on the basis that the author and publisher accept no responsibility for any loss, damage, cost or expense arising directly or indirectly from the use of any information or other material contained in the report.

This report is not investment advice. It should not be relied on for such advice or as a substitute for professional accounting, tax, legal, financial or other advice as appropriate. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities.

PaymentsCM LLP

The Stable Yard, Kelling Estate

Kelling, Norfolk, NR25 7EW

Tel: + 44 (0) 1263 711937

www.paymentscardsandmobile.com

NCR

NCR Corporation

3097 Satellite Boulevard

Duluth, Georgia 30096, USA

www.ncr.com

PAYMENTS INDUSTRY INTELLIGENCE
Payments
CARDS & MOBILE

NCR